# Department of Homeland Security
# Information Analysis and Infrastructure Protection
# Daily Open Source Infrastructure Report for 18 June 2003

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
www.whitehouse.gov/homeland

## Daily Overview

- CBS News reports U.S. postal inspectors throughout the West are waging a new campaign against identity theft: tracking down scores of suspected mail thieves who steal credit cards, Social Security numbers, and bank accounts, which provide the raw materials for criminals to steal whole identities. (See item 5)
- The Department of Homeland Security: Customs & Border Protection announced the opening of a new rail inspection building in Laredo, Texas, which includes a gamma−ray imaging system for scanning cargo in rail cars in order to combat illegal migrant and drug smuggling on trains, as well the smuggling of terrorists and weapons of mass destruction. (See item 9)
- vnunet reports several third−party device drivers that ship with Windows Server 2003 contain a vulnerability that causes them to leak potentially sensitive data during TCP transmissions. (See item 23)

**DHS/IAIP Update *Fast Jump***

**Production Industries:** Energy; Chemical; Defense Industrial Base
**Service Industries:** Banking and Finance; Transportation; Postal and Shipping
**Sustenance and Health:** Agriculture; Food; Water; Public Health
**Federal and State:** Government; Emergency Services
**IT and Cyber:** Information and Telecommunications; Internet Alert Dashboard
**Other:** General; DHS/IAIP Web Information

# Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 17, New York Times* — **Short supply of natural gas is raising economic worries.** The economy has been cool, and so has the spring in much of the country. Nonetheless, the United States is facing its most severe shortage of natural gas in a quarter−century. **Industries like fertilizer and ammonia makers, which use gas to produce their goods, are already laying off workers. And experts warn that a warming trend, in the economy or the weather, could send prices spiking for the electricity that cools homes and runs every sort of**

**business.** Most analysts agree, the basic law of supply and demand is at work. **With natural gas promoted as a cleaner−burning fuel than oil or coal, nearly all the electric plants built since 1998 are designed to be fired mainly by gas. So demand is up.** And while drilling has increased about 25 percent in the last year, much of it has been confined to old, overworked basins that are not as productive as they once were. Supplies, therefore, have not kept up. **Prices for natural gas have risen sharply in the last year, reaching a peak at more than $6 per million British thermal units, compared with about $3.65 a year earlier.** Stored supplies of natural gas have fallen to the lowest level since the federal government began keeping records in 1976, with levels about 30 percent below the average for the last five years. Source: http://www.nytimes.com/2003/06/17/business/17GAS.html

2. *June 15, Associated Press* — **Mexican power plants begin operations amid U.S. legal fight.** A sprawling 37−acre (15−hectare) display of tubes and silos is supplying electricity to thousands of homes in the western United States, but this power plant is not even on U.S. soil. It's in northern Mexico's desert, just three miles (5 kilometers) from the border. The plant's owner, San Diego−based Sempra Energy, says it found an ideal site, with open land, water, fuel and transmission line capacity. **Environmentalists say Sempra, and the owners of a second plant nearby, built them in Mexico to avoid U.S.−mandated pollution controls.** They argue that the plants threaten to contaminate water and air across the region. Sempra's US$350 million plant is currently sending power to the United States in test runs; **it plans to start commercial operations to 600,000 customers this summer.** The second plant, a US$750 million facility built by InterGen, a joint venture of Bechtel Group Inc. and Royal Dutch/Shell Group, **will produce enough power to light up one million homes on both sides of the U.S.−Mexican border.** Environmentalists opposing the plants have taken their fight to court, charging the plants violate the National Environmental Protection Act and other federal rules. Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=ap_2003_06_15_−−−−−_1822−1709−LA−GEN−−Mexico −Border.a>

[Return to top]

## Chemical Sector

Nothing to report.
[Return to top]

## Defense Industrial Base Sector

3. *June 17, Reuters* — **War on terror accelerates world military spending.** World military spending rose by six percent last year, growing twice as fast as in 2001 to reach $794 billion, largely as a result of the U.S.−led war on terrorism, a respected think−tank said Tuesday. **Washington accounted for three quarters of the increase, the Stockholm International Peace Research Institute (SIPRI) said in its Yearbook, a defense and security policy publication widely recognized for the reliability of its data.** But with outlays up 10 percent year−on−year at $336 billion, the United States accounted for 43 percent of global military expenditure in 2002, up from 36 percent in 2001. "The rest of the world is not prepared, or cannot, follow the USA's example in increasing military expenditure," SIPRI said, noting that

combined arms expenditure of the West European members of the NATO defense alliance fell by three percent in real terms between 2000 and 2002. **"While in the USA the war on terrorism was a major factor in the huge growth in military expenditure in 2002, this was not the case in Europe."**
Source: http://www.washingtonpost.com/wp−dyn/articles/A3787−2003Jun1 7.html

[Return to top]

## Banking and Finance Sector

4. *June 17, USA Today* — **Pickpockets may have eye on you.** Pickpockets may not draw as much attention as more brutal crooks. But they still wreak damage on their victims. In 2001, more than 158,000 people nationwide lost $45 million to pickpockets, according to the Justice Department. In recent years, pickpockets and their crews have grown in scope and sophistication, he says. They're no longer clumsy street thugs but slick operators who pride themselves on playing the "game" and "scoring" − stealing a wallet or pocketbook unnoticed, without a gun or knife. **More pickpockets are hooking up with crooks who run fast−growing identity theft scams. Pickpocket gangs will lift credit cards, driver's licenses and Social Security cards from wallets and purses, then deliver the goods to the identity thieves.**
Source: http://www.usatoday.com/money/biztravel/2003−06−16−pickpocke ts_x.htm

5. *June 17, CBS News* — **Cracking down on identity theft. Waging a new campaign against identity theft, U.S. postal inspectors throughout the West are tracking down scores of suspected mail thieves.** "At this time 96 suspects have been apprehended throughout northern California, and that continues to grow," said U.S. Postal Service spokesman John Wisniewski. **Officials announced Tuesday that what was stolen from mailboxes, credit cards, Social Security numbers, bank accounts, provided the raw material for criminals to steal whole identities. "The fact of the matter is that one's mail is a veritable treasure trove for would−be identity thieves,"** says Larry Brown, assistant U.S. Attorney for the Eastern District of California. **Last year the Federal Trade Commission received more than 160,000 complaints from victims of identity theft. The Post Office says the first line of defense is to pick up your mail before someone else does.**
Source: http://www.cbsnews.com/stories/2003/06/17/eveningnews/main55 9115.shtml

6. *June 16, U.S. Department of the Treasury* — **Study of the potential effects of acts of terrorism on the availability of other lines of insurance. The terrorism insurance legislation enacted on November 26, 2002, requires the Secretary of the Treasury, after consultation with the National Association of Insurance Commissioners (NAIC), representatives of the insurance industry, and other experts in the insurance field, to conduct a study of the potential effects of acts of terrorism on the availability of life insurance and other lines of insurance coverage, including personal lines, and to submit a report to the Congress on the results of the study by August 26, 2003.** To assist in the study, the Treasury is soliciting comments on the questions listed under the following: I. Exposure of Insurance Lines Not Covered Under Section 102(6) of the Act to Acts of Terrorism Defined in Section 102(1) of the Act; II. Current Insurance Availability Conditions; and III. Impact of Potential Future Acts of Terrorism.

Source: http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03−15074.htm

7. *June 16, U.S. Secret Service* — **United States Secret Service forms new task forces.** The United States Secret Service has announced the formation of four new Electronic Crimes Task Forces, a sucessful public−private partnership aimed at fighting high−tech computer−based crimes. The new task forces will open in Dallas, Houston, Cleveland, and Columbia, South Carolina, and join an existing network of nine other nationwide operations. **"Our goal is to keep our community and nation safe against various forms of electronic crimes and terrorist attacks against the critical infrastructure and financial payment systems,"** said Secret Service Director Ralph Basham. "These task forces are about sharing information and resources in an effort to enhance our strengths and minimize our weakness against those that would do us harm." **The types of investigations handles by the task forces encompass a wide range of computer−based criminal activity. Examples include e−commerce frauds, intellectual property violations, identity crimes, telecommunications fraud, and a wide variety of computer intrusion crimes that affect a variety of infrastructures.**
Source: http://www.secretservice.gov/press/pub1903.pdf

[Return to top]

## Transportation Sector

8. *June 16, v* — **More security at Penn Station. Upgrading of anti−terrorist security in the century−old tunnels of Pennsylvania Station is on track but much more money is needed to complete the job,** Sen. Charles Schumer (D−NY) said Monday. Schumer said $77 million of an original $100 million allocated for the project has been spent and another $350 million will be required. He spoke after a tour of the facilities with Asa Hutchinson, the undersecretary of the Department of Homeland Security. Their tour was designed to examine the changes that have been made since September 11, 2001, and what remains to be accomplished in the nation's busiest railroad station. Schumer said **the money has been used for sensors to detect chemical, biological and radioactive threats and explosives, intrusion alarms and an extensive television monitoring system covering all entrances at the sprawling station,** which is owned by Amtrak and also serves New Jersey Transit and the Long Island Rail Road. **The further improvements would include three major air ventilation systems, a fire standpipe network and escape routes in the tunnels, some of which are two to three miles long.** Penn Station is used by some 400,000 local commuters and long−distance train travelers each day.
Source: http://www.newsday.com/news/local/newyork/nyc−penn0617,0,2196056.story?coll=ny−nynews−headlines

9. *June 12, Department of Homeland Security: Customs &Border Protection* — **CBP, Mexican customs, rail officials dedicate new rail inspection building.** Jayson Ahern, Assistant Commissioner of Customs and Border Protection (CBP), Lic. Leopoldo Perea Cardenas, Administrador de Aduanas de Nuevo Laredo, and several top railroad officials today dedicated a state−of−the−art rail cargo inspections facility at Laredo, Texas, on the U.S.−Mexico border. **The new facility houses BCBP rail inspection operations, including a gamma−ray imaging system for scanning cargo in rail cars. The $200,000 facility, built by Tex−Mex Railroad**

**on land owned by Union Pacific, houses offices for CBP inspectors and Border Patrol agents, and a $1.3 million gamma−ray imaging system that scans railcars as they cross into the U.S.** The new two−story structure replaces an outmoded facility at the border rail crossing dating back to 1908. Assistant Commissioner Ahern said, "Co−location of CBP inspectors and Border Patrol agents, along with cutting−edge technology, will enhance both efficiency and effectiveness in combating illegal migrant and drug smuggling on trains, as well the smuggling of terrorists and weapons of mass destruction."
Source: http://www.cbp.gov/xp/cgov/newsroom/press_releases/06122003. xml

10. *June 04, SignOnSanDiego.com* — **Plans announced for 24−hour entry at Otay Mesa border crossing.** Federal officials announced plans today to expand incrementally the hours Otay Mesa Port of Entry is open, making the border crossing facility available to passenger traffic 24 hours a day this summer. **Starting June 15, those leaving or entering Mexico at the southeastern San Diego complex will have four more hours a day to do so, from 4 a.m. to midnight, according to the U.S. Bureau of Customs and Border Protection.** Under that schedule, the processing and inspection station will open two hours earlier each morning and close two hours later each night than it does now, said Adele Fasano, interim local BCBP field operations director. The two−step approach will allow the 13−lane facility's management to adjust its staffing and operational procedures smoothly, she added. **The complex is eight miles east of the world's busiest port of entry, located in San Ysidro.**
Source: http://www.signonsandiego.com/news/metro/20030604−1419−borde rhours.html

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

11. *June 17, Wisconsin Ag Connection* — **Final mad cow quarantines lifted. Quarantine orders on the final four farms in the mad cow disease or BSE investigation have been lifted. The Canadian Food Inspection Agency says tests on a final 700 animals have failed to turn up any new cases of BSE.** CFIA spokesman Dr. Claude Lavigne acknowledged that investigators may never nail down the source of the infection. Ted Haney, president of the Canadian Beef Export Federation, says it's possible the U.S. could open its borders to some Canadian beef products this week. **Haney says Mexico is also getting "closer and closer" to reviewing its ban, while Japan and South Korea have sent technical teams to Canada to review Canadian mad cow standards and could open their borders in two weeks.**
Source: http://www.wisconsinagconnection.com/story−national.cfm?Id=6 65t>

12. *June 17, Press Telegram* — **Exotic Newcastle cases are now few. After seven months and 3.5 million birds destroyed, agriculture officials say they are getting a handle on Exotic Newcastle disease in Southern California.** Eradication teams are still going door−to−door examining poultry, parrots, and other pet birds for signs of the highly contagious virus. **They**

**reported only four new infections in May and none so far in June. Officials hope to remove the quarantine in Ventura, Santa Barbara, and Imperial counties if the next round of testing comes up clean.** The outbreak was discovered last October in Compton, among a backyard flock of chickens.
Source: http://www.presstelegram.com/Stories/0,1413,204~21474~145972,7,00.html

[Return to top]

## Food Sector

**13.** *June 17, Food Production Daily* — **FSA releases Campylobacter strategy.** The Food Standards Agency (FSA) Tuesday publishes for consultation its strategy to tackle the problem of Campylobacter in UK−produced chicken. The organism is said to be the single biggest cause of foodborne illness in the UK. **Last year an FSA survey found Campylobacter in around 50 percent of chicken on retail sale in the UK. The main focus of the strategy will be improving farm biosecurity measures, but it also considers options for control at poultry processing plants.** Work carried out by the agency shows that, while biosecurity across the industry is generally good, there is a need to tighten up some areas and follow best practice, with particular attention to the provision of handwashing facilities, better control over access to the broiler house, and the movement of equipment between broiler houses.
Source: http://www.foodproductiondaily.com/news/news.asp?id=2981

[Return to top]

## Water Sector

**14.** *June 17, KGTV TheSanDiegoChannel.com* — **Water supply shortage may hit San Diego.** This past winter, 10 inches of rain fell on San Diego, CA. The rain helped refill some of the lakes and reservoirs. However, it did little to help San Diego through an impending emergency. **If a string of hot days hits San Diego this summer, there is a good chance there will be a water shortage.** "We will ask folks to take radical steps to save the water supply. **Ninety percent of our water comes from elsewhere and it must be heavily treated," said Bill Jacoby of the San Diego County Water Authority. Apparently the treatment capacity has fallen way behind at local facilities. It will take five years and a lot of construction to get the water supply up to where it should be.** "There are a number of plants being expanded. It will take some time and there will days when the county will have a hard time meeting the demand," Jacoby said. In Carlsbad, Olivenhain, Scripps Ranch, and other places around the county, about six new water treatment facilities are being designed and built.
Source: http://story.news.yahoo.com/news?tmpl=story_3/lo_kgtv/1657351

**15.** *June 17, Associated Press* — **Water at Erie Shriners hospital tested for Legionnaires' disease.** Health officials are testing water samples from Erie Shriners Hospital for Children, in Pennsylvania, because a hospital security guard who died June 6 tested positive for Legionnaires' disease. **Results of the hospital water tests are expected within a week.** The hospital remained open Tuesday and patients were not at risk, said Dr. Sandra Fortna, the hospital's director for infection control. No other patients have contracted the disease, nor have

any staff. **If the bacteria is found at the hospital, it can likely be remedied by treating the tainted water source, which would not require the hospital to close, county health officials said.**
Source: http://pennlive.com/newsflash/pa/index.ssf?/base/news−3/1055 856845110650.xml

16. *June 16, KUSA TV Denver* — **Senator asks Congress for money to fight water−guzzling plant. Senator Ben Nighthorse Campbell is asking Congress for $20 million to eradicate a water−guzzling, non−native plant from Colorado and other southwestern states.** The tamarisk a hard−to−kill shrub is flourishing along Colorado riverbanks. **One plant can absorb up to 300 gallons of water a day. In Colorado, tamarisk consumes an estimated 250,000−acre feet of water a year; about the same amount that Denver Water provides to its customers annually.** Tamarisk is resistant to disease and has no natural enemies in the U.S. Representative Scott McInnis has also asked Congress for $1 million to fund long−range eradication research, and Senator Pete Domenici plans to reintroduce a bill this year that could make more than $10 million available annually for tamarisk control in Colorado and five other Southwestern states.
Source: http://www.9news.com/storyfull−newsroom.asp?id=15465

[Return to top]

## Public Health Sector

17. *June 17, Reuters* — **AMA tackles emergency preparedness. The American Medical Association (AMA) on Monday unveiled a basic disaster life support (BDLS) program aimed at rapidly training physicians, nurses, and emergency medical technicians for all disasters.** The new curriculum will be ready "by August, and by this time next year we expect it to be offered at training centers nationwide," Dr. James J. James said. The new disaster−training curriculum is a cooperative effort of the AMA, the U.S. Department of Health and Human Services, the Medical College of George, and University of Texas Southwestern. **Among the topics covered in the course are traumatic and explosive events, natural and man−made disasters, biological events, chemical events, medical decontamination, legal issues of disaster response, and media and communications during disasters.**
Source: http://reuters.com/newsArticle.jhtml?type=healthNews=2942420

18. *June 17, MSNBC* — **WHO lifts Taiwan SARS advisory. The World Health Organization (WHO) on Tuesday canceled its warning against travel to Taiwan, more than a month after it put the Taiwanese capital on its list of places with a risk of spreading Severe Acute Respiratory Syndrome (SARS).** WHO said its decision to remove the travel warning in Taiwan "follows vast improvements in case detection, infection control, and the tracing and follow−up of contacts that led to a steep drop in the daily number of new cases." The organization based its decision to end the travel advisory on several criteria, including the number of new cases, patterns of local transmission, and evidence that cases are no longer being exported elsewhere. **Taiwan's removal leaves Beijing as the only area on the travel warning list.**
Source: http://www.msnbc.com/news/885653.asp?0cv=CB10

19. *June 01, Federal Register* — **Cooperative research and development agreement. The Division of Bacterial and Mycotic Diseases (DBMD) at the U.S. Centers for Disease Control and Prevention (CDC) is seeking to explore possible partnerships in applied research to improve public health preparedness and response to bioterrorism associated with use of bacterial and fungal agents.** Bioterrorism−related research of interest to the DBMD includes: rapid evaluation of powder, food, water, and other potential vehicles for presence of bioterrorism agents; epidemiologic investigation of suspected and confirmed bioterrorism events; bioterrorism event surveillance; diagnosis of suspect and confirmed bioterrorism−related illness; treatment of suspect and confirmed bioterrorism−related illness; post−exposure prophylaxis for prevention of bioterrorism−related illness among exposed persons; and remediation of health risks in environments contaminated or potentially contaminated as a result of bioterrorism events. **The division works in partnership with a variety of public, academic, and for−profit and not−for−profit private sector organizations to achieve public health goals.**
Source: http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03−15218.htm

[Return to top]

## Government Sector

20. *June 17, Associated Press* — **ATF Opens New Crime and Research Lab.** The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) opened new crime and research laboratories Monday at a center that will be used to trace guns used in crimes, recreate suspicious fires and track the origins of bombs. **The $106 million, 176,000−square−foot suburban Washington center replaces the ATF's cramped and aging Rockville lab, which was used in investigations including the Washington−area sniper shootings and the Oklahoma City bombing.** The National Laboratory Center, which took eight years to complete, will significantly increase the scientific capabilities of the bureau, said ATF Director Bradley Buckles.
Source: http://www.washingtonpost.com/wp−dyn/articles/A2962−2003Jun1 6.html

[Return to top]

## Emergency Services Sector

Nothing to report.
[Return to top]

## Information and Telecommunications Sector

21. *June 14, BBC News* — **India gears up to fight hackers. India's first internet security centre is due to become operational in July. The centre will aim to prevent cyber attacks on key defense, business and government establishments. The project is being handled by the central information technology ministry with the help of the U.S.−based security group, CERT**, a research and development centre run by the Carnegie Mellon University. The date for

the launch of the net security centre was announced by India's Information Technology Secretary Rajiv Ratan Shah in the southern Indian city of Bangalore. Based in the capital, Delhi, the centre is expected to cost up to $20 million. A second centre will be set up in Bangalore at India's leading research organization, the Indian Institute of Science.
Source: http://news.bbc.co.uk/2/hi/technology/2988604.stm

**22.** *June 13, internetnews.com* — **Pentagon commits to IPv6.** The Pentagon announced Friday it is beginning a transition to Internet Protocol Version 6 (Ipv6) to bring the Department of Defense (DoD) closer to its goal of net−centric warfare and operations. **The new protocol will facilitate integration of the essential elements of DoD's global information grid, including its sensors, weapons, platforms, information and people**. The current version of the Internet's operating system, IPv4, has been in use by DoD for almost 30 years. Its fundamental limitations, along with the world−wide explosion of Internet use, inhibit net−centric operations. **IPv6 is designed to overcome the limitations of IPv4, such as the limited number of available IPv4 addresses and adds improvements to IPv4 such as routing and networking autoconfiguation**. After a period of coexistence, IPv6 is expected to replace IPv4 as the standard system for the Internet. Assistant Secretary of Defense John P. Stenbit signed a policy memorandum on June 9 outlining a strategy that aims to ensure an "integrated, timely and effective transition."
Source: http://www.internetnews.com/infra/article.php/2221821

**23.** *June 13, vnunet* — **Flaws expose Win Server 2003. Several third−party device drivers that ship with Windows Server 2003 contain a vulnerability that causes them to leak potentially sensitive data during TCP transmissions**. Security experts have criticized many of the vendors for failing to act quickly enough to guide users to fixes, and warned that **the flaw could lead to attacks through local area networks** (LANS). The so−called Etherleak flaw, first identified in January, occurs when messages transmitted between two machines are padded with arbitrary data in order to bring their byte size in line with the accepted standard. Chris Taget of security consultancy NGS Software warned that the vulnerability could be extremely serious and suggested that "**IT directors should find out whether their vendors have updated the driver to resolve the issue**."
Source: http://www.vnunet.com/News/1141591

## Internet Alert Dashboard

### Current Alert Levels

| | |
|---|---|
| AlertCon: 1 out of 4<br>https://gtoc.iss.net | Security Focus ThreatCon: 1 out of 4<br>http://analyzer.securityfocus.com/ |

### Current Virus and Port Attacks

| | |
|---|---|
| **Virus:** | |

| | |
|---|---|
| | #1 Virus in the United States: **WORM_LOVGATE.F**<br>Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States] |
| **Top 10 Target Ports** | 137 (netbios−ns), 80 (www), 1434 (ms−sql−m), 445 (microsoft−ds), 113 (ident), 139 (netbios−ssn), 4662 (eDonkey2000), 0 (−−−), 2234 (directplay), 53 (domain)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

[Return to top]

## General Sector

**24.** *June 17, Reuters* — **Britain: attack on western city "matter of time". A terror attack on a major Western city using chemical, biological, radiological or nuclear technology (CBRN) is "only a matter of time," the head of Britain's domestic intelligence service MI5 said Tuesday.** Eliza Manningham−Buller said violent extremists were becoming more sophisticated in developing such non−conventional threats thanks to help from "renegade scientists." **"We are faced with the realistic possibility of some form of unconventional attack. That could include a CBRN attack," she told a conference in London on countering terrorism.** "Sadly, given the widespread proliferation of the technical knowledge to construct these weapons, it will only be a matter of time before a crude version of a CBRN attack is launched at a major Western city," she added. **The MI5 head was not referring to any specific new threat and was only repeating previous warnings from intelligence sources. But such blunt words in public from a senior secret service official are rare.**
Source: http://www.nytimes.com/reuters/international/international−s ecurity−britain.html

**25.** *June 17, Ascribe Newswire* — **Online master's degree trains managers to anticipate, prepare for terrorism.** The University of Washington is planning to offer a new online master's degree this fall, designed to prepare students for leadership in homeland security issues. **The online Master's in Strategic Planning for Critical Infrastructure is a 45−credit program that will prepare managers and other professionals to protect transportation systems, electrical grids, water systems and other essential infrastructure from terrorist attacks and other hazards.** "This program analyzes infrastructure to make it less susceptible to any kind of threat," said Hilda Blanco, chair of the UW Department of Urban Design and Planning. "The emphasis is on ways that enable you to make those systems more resilient in the future." The courses in the program have been designed by the UW's College of Architecture and Urban Planning and the School of Public Health and Community Medicine. **They focus on hazards such as biological and chemical attacks, with strong concentrations in geographic information systems, strategic planning and data analysis. Students will also get a solid grounding in legal and ethical issues regarding homeland security.**
Source: http://www.ascribe.org/cgi−bin/spew4th.pl?ascribeid=20030617 .101026DT=1

[Return to top]

## DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

### DHS/IAIP Daily Open Source Infrastructure Report Contact Information

| | |
|---|---|
| Content and Suggestions: | nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202−324−1129 |
| Distribution Information | Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information. |

### Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

### DHS/IAIP Disclaimer